Problem 10: Caesar Cipher

Points: 20

Author: Steve Gerali, Denver, Colorado, United States

Problem Background

The Caesar Cipher is one of the earliest known ciphers, and among the simplest to learn. It is a "substitution cipher", in which each letter in the original message (the "plaintext") is shifted a certain number of places down the alphabet. For example, with a shift of 1, an A would be replaced with a B, a B would be replaced with a C, and so on. This method is named after Julius Caesar, who apparently used it to communicate with his generals.

To pass an encrypted message from one person to another, it is necessary that both parties have the "key" for the cipher, so that the sender can encrypt it and the recipient can decrypt it. For the Caesar Cipher, the key is the number of letters by which to shift the cipher alphabet.

Problem Description

You are working for the History Channel, who wants to decrypt all communications that Julius Caesar made to his generals in order to support a new documentary they're filming about the Roman emperor. You will be given a list of encrypted messages, and the key believed to be used to encrypt those messages. Your program must decrypt those messages.

For the purposes of this problem, we will be using the English alphabet, shown below in its standard order (with a shift of 0).

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

If encrypting a message with a shift of 1, each letter in the plaintext will be replaced with the respective letter shown in the 1-shifted alphabet below.

B C D E F G H I J K L M N O P Q R S T U V W X Y Z A

To decrypt a message, the process is reversed; a letter in the ciphertext would be replaced with the respective letter in the original English alphabet.

Spaces are not encrypted in this cipher and should remain in place when decrypting a message.

Page 2

Sample Input

The first line of your program's input, **received from the standard input channel**, will contain a positive integer representing the number of test cases. Each test case will include two lines:

- A line with a single integer representing the message key - the number of letters by which to shift the alphabet when encrypting the message.
- A line containing lowercase letters and spaces, representing the encrypted message.

3
1
buubdl bu ebxo
3
ghvwurb wkh fdvwoh
6

yzkgr znk ynov

Sample Output

For each test case, your program must output the decrypted message. Messages should be printed in lowercase, and all spaces should be retained.

attack at dawn

destroy the castle

steal the ship

Sample Output